X.509 Certification Practices Statement for the U.S. Government Printing Office Subordinate Certification Authority (GPO-SCA)

June 15, 2007

FINAL

Version 1.6.1

FOR OFFICIAL USE ONLY

SIGNATURE PAGE

_____ _____

U.S. Government Printing Office DATE

Public Key Infrastructure Operating Authority

_____ _____

U.S. Government Printing Office DATE

Public Key Infrastructure Policy Authority Chair

TABLE OF CONTENTS

RECORD OF CHANGES

Version	Date	Author(s)	Reason	Description
1.0	December 9, 2003	CygnaCom Solutions	Initial Document	Initial Document
1.1	March 22, 2004	CygnaCom Solutions	Policy correction	Refine badge requirements for personnel filling GPO PKI Trusted Roles.
1.2	November 9, 2004	CygnaCom Solutions	Changes based on CP update	Address text modified in the CP
1.2.1	November 11, 2004	CygnaCom Solutions	Changes CP/CPS mapping	Align section numbering and address issues that may arise during an audit
1.2.2	November 11, 2004	CygnaCom Solutions	Correcting possible audit issues	
1.3	July 8, 2005	U.S. Government Printing Office	Responding to audit comments.	Minor changes. Removed Confidentiality Statement, added “For Official Use Only” classification to the document, and various other changes based on audit comments received from SeNet International Corporation.
1.4	February 27, 2006	U.S. Government Printing Office	Changes to comply with Federal PKI Common Policy and PKI Shared Service Provider (SSP) requirements	Changes to various sections required to comply with Common Policy requirements.
1.5	July 1, 2006	U.S. Government Printing Office	Changes to comply with AICPA WebTrust for CA auditor and GPO OIG audit recommendations.	Changes to various sections based on WebTrust for CA auditor and GPO OIG audit recommendations.
1.6	August 3, 2006	U.S. Government Printing Office	Minor changes to comply with GPO OIG and AICPA WebTrust for CA auditor recommendations.	Minor changes to a few sections based on GPO OIG and WebTrust auditor recommendations.
1.6.1	June 15, 2007	U.S. Government Printing Office	Clarifications on RA requirements for external RA’s to comply with GPO OIG and AICPA WebTrust for CA auditor recommendations.	Minor changes to a few sections to address the GPO OIG and AICPA WebTrust auditor recommendations.

1. INTRODUCTION

The Government Printing Office (GPO) is implementing a comprehensive Public Key Infrastructure (PKI) to provide the services necessary to enable the use of authentication, encryption, and digital signatures to secure GPO systems, communications, applications and data, and to enable the automation of inefficient and costly paper processes.

The PKI will provide Medium Assurance level certificates as defined in the GPO Certificate Policy (GPO CP). The PKI consists of products and services that provide and manage X.509 certificates for public key cryptography. Part of this PKI is a Certification Authority (CA) that generates and revokes X.509 public key certificates. The CA binds the Subscribers to their public/private key pairs, through the issuance of X.509 certificates.

The GPO PKI will consist of an air-gapped Root /Principal CA (PCA) and one, or more, Subordinate CAs (SCA). The GPO CP defines the requirements for the creation and management of Version 3 X.509 public-key certificates. This Certification Practices Statement (CPS) defines the practices under which the Medium Assurance GPO Subordinate CA (GPO-SCA) will operate. This CPS is applicable to all Subscribers, Relying Parties, and Registration Authorities of the GPO-SCA. This CPS provides these entities with a clear statement of the practices and responsibilities of the GPO-SCA, as well as the responsibilities of each entity in dealing with the GPO-SCA.

Security management services provided by the GPO-SCA include:

- Key Generation/Storage/Recovery
- Certificate and Certificate Revocation List (CRL) Generation and Distribution
- Certificate Update, Renewal, and Re-key
- Certificate token initialization/programming/management
- System Management Functions (e.g., security audit, certificate tracking, archive, etc.)

The security and trustworthiness of the GPO-SCA depends on the security of the equipment, software, facilities, personnel, and procedures used in the operation of the GPO-SCA.

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

The practices specified in this CPS may be described in more detail in a PKI Operating Procedures document.

1.1 OVERVIEW

Certificates from the GPO-SCA may be issued to all GPO employees and contractors, and to GPO systems and application processes, as required. Certificates may also be issued to non-GPO personnel using GPO applications. GPO intends to offer PKI as a service to other Agencies, who would issue certificates to employees, contractors and any other people the Agency may require certificates to work with. Encryption, authentication, and digital signature in support of non-repudiation key pairs will be supported. FIPS 140 certified software and hardware cryptographic modules will be used.

This version of the CPS provides for the issuance of Subscriber certificates to all Subscribers of the GPO-SCA.

1.1.1 Certificate Policy

The practices described in this CPS are governed by and have been developed to support the GPO CP. The requirements in this CPS add to those in the CP. The GPO CP is incorporated into this document by reference.

1.1.2 Relationship Between the GPO CP and this CPS

Where the CPS is compliant with the GPO CP and does not add to it, the phrase "As stipulated in the GPO CP" is used. Where the GPO CP specifies "No stipulation" and the CPS does not add to it, the phrase "No stipulation" is used.

1.1.3 External CA Interoperation

As stipulated in the GPO CP.

1.2 IDENTIFICATION

This document is known as the GPO Subordinate Certification Authority Certification Practices Statement**.**

The practices stated herein conform to the specifications as defined in the GPO CP.

The GPO-SCA will be responsible for issuing certificates to all approved Subscribers, services, applications and devices. Certificates that are created using these practices will assert the following policy Object Identifier (OID):

id-gpo-certpcy-mediumAssurance	::= {2 16 840 1 101 3 2 1 17 1}

The CA automatically populates the appropriate OID in certificates.

1.3 COMMUNITY AND APPLICABILITY

1.3.1 PKI Authorities

1.3.1.1 GPO PKI Policy Authority (PA)

As stipulated in the GPO CP.

1.3.1.2 GPO Operational Authority (OA)

The GPO-SCA has an Operational Authority as defined in the GPO CP.

1.3.1.3 GPO Operational Authority Oversight Administrator

As stipulated in the GPO CP.

1.3.1.4 GPO Operational Authority Officers

As stipulated in the GPO CP.

1.3.1.5 Entity Certification Authority

As stipulated in the GPO CP.

1.3.1.6 GPO Certification Authority

As stipulated in the GPO CP.

1.3.1.6.1 GPO Root / Principal Certificate Authority (PCA)

The GPO-PCA is the apex of the GPO PKI hierarchy.

1.3.1.6.2 GPO Subordinate Certificate Authority (SCA)

The GPO-SCA is subordinate to the GPO-PCA.

1.3.1.7 GPO Naming Authority

As stipulated in the GPO CP.

1.3.1.8 GPO Registration Authority (RA)

As stipulated in the GPO CP.

1.3.2 Related Authorities

1.3.2.1 Federal Bridge Certification Authority (FBCA)

As stipulated in the GPO CP.

1.3.3 End Entities

1.3.3.1 Subscribers

As stipulated in the GPO CP.

1.3.3.2 Relying Parties

As stipulated in the GPO CP.

1.3.3.3 PKI Sponsor

As stipulated in the GPO CP.

1.3.4 Applicability

The GPO-SCA is responsible for issuing GPO Medium Assurance Certificates to all approved Subscribers, services, applications and devices.

1.3.4.1 Usage Determination

The Relying Party must determine if the certificates issued under the GPO-CAs are appropriate for their application. This may be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the GPO-PA or the GPO-OA.

1.3.4.2 Authorized Applications

Authorized applications are approved for the following security services provided by the GPO PKI:

- User Authentication
- Logical Access Control
- Secure Communication
- Digital Signature/Non-repudiation

The GPO PA may identify additional authorized applications. This CPS will be updated as new authorized applications are identified.

1.3.4.3 Prohibited Applications

Applications that attempt to use these certificates for services other than those identified are prohibited.

1.4 CONTACT DETAILS

1.4.1 Specification Administration Organization

The GPO-SCA OA is responsible for all aspects of this CPS.

1.4.2 Contact Information

Questions regarding this CPS shall be directed to the Chair of the GPO-PA, whose address can be found at http://www.gpoaccess.gov/pki

1.4.3 Person Determining CPS Suitability for the Policy

As stipulated in the GPO CP.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

The obligations described below pertain to the GPO-SCA and operations personnel.

2.1.1 CA Obligations

As stipulated in the GPO CP.

2.1.2 RA Obligations

The RA will abide by all obligations defined in the GPO CP for Medium assurance certificates by following the procedures defined in this CPS.

2.1.3 Subscriber Obligations

Subscriber obligations are specified in the Subscriber agreement that each Subscriber applicant must sign prior to the time they receive their keys and certificates.

2.1.4 Relying Party Obligations

As stipulated in the GPO CP.

2.1.5 Repository Obligations

As stipulated in the GPO CP.

2.1.6 Certificate Issuance to Non-GPO Parties

The GPO-CA may issue certificates as established by the GPO-PA. A Subscriber Agreement or similar instrument will be executed, and will contain whatever provisions are determined appropriate by the GPO-PA. All subscribers will be registered as described below in Section 3.1.9, Authentication of Individual Identity.

2.2 LIABILITY

As stipulated in the GPO CP.

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Indemnification by Relying Parties and Subscribers

No stipulation.

2.3.2 Fiduciary Relationships

No stipulation.

2.3.3 Governing Law

As stipulated in Section 1 of the GPO CP.

2.3.4 Administrative Processes

Administrative processes pertaining to this CPS shall be determined by the OA pursuant to the agreement between it and the GPO PA for the operation of the GPO-SCA.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that any relevant section of the GPO CP is incorrect or invalid, all parties with certificates issued by the GPO-SCA will nevertheless abide by the practices as described in this CPS, until guidance is given for new policy and a new CPS is drafted.

2.4.2 Dispute Resolution Procedures Imposed on Subscribers

The PA resolves any disputes over the interpretation or applicability of the CPS.

2.5 FEES

As stipulated in the GPO CP.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of CA Information

The OA will deliver its CPS to the PA for approval. As stipulated in the GPO CP, this CPS will not be published in the Repository. Upon direction from the PA, the OA may make the CPS available under a non-disclosure agreement, in whole or in part, to other entities with a need-to-know.

The GPO-SCA will publish the following information to the repository:

- All encryption certificates issued by the GPO-SCA
- All CRLs issued by the GPO-SCA
- The GPO-SCA CA certificate

2.6.2 Frequency of Publication

Certificates are published in the directory as they are issued. CRLs and ARLs are published in the directory as they are issued.

The automated replication mechanism used internal to the Directory is configured to replicate any changes as the changes occur.

2.6.3 Access Controls

Only the PA has permission to modify, replace or remove this CPS. The PA may delegate some or all of this responsibility to the OA.

All Subscribers who have been issued certificates by the GPO-SCA have read-only access to a copy of the GPO CP through the GPO web site.

The Master Directory and the Shadow Directories reside on the GPO internal network behind one or more GPO controlled firewalls; all GPO users shall have read-only access to the individual entries in the Shadow Directories.

The GPO-SCA application generates certificates and CRLs and has read, write and delete privileges to the master directory for PKI attributes. Directory Administrators and OA Officers have read, write and delete access for PKI-related attributes associated with individual entries in the master directory. The Master Directory information is automatically replicated to the shadow directories.

These access controls will be set with the native access control mechanisms of the Directory.

2.6.4 Repositories

The repository for the GPO-SCA is an X.500 Directory and is accessed using the Lightweight Directory Access Protocol (LDAP) version 3, as specified in Internet RFC 1777.

2.7 COMPLIANCE AUDIT

2.7.1 Frequency of Entity Compliance Audit

Internal compliance audits shall be performed according to the following schedule: prior to initial approval of the GPO-SCA, and once every 12 months thereafter.

2.7.2 Identity/Qualifications of Compliance Auditor

The GPO PA will have the responsibility to verify that the compliance auditor selected, by the GPO-OA, to audit the SCA and any applicable personnel meet the requirements governing the identity and qualifications of the compliance auditor that are stipulated in the GPO CP.

2.7.3 Compliance Auditor's Relationship to Audited Party

The compliance auditor is a firm in a contractual relationship with the GPO and has no GPO PKI management capabilities or responsibilities.

2.7.4 Topics Covered by Compliance Audit

The compliance audit verifies that the operational and technical controls used by the GPO-SCA operations personnel satisfy all stipulations in this CPS, including the following topics:

- Identification & Authentication (Section 3)
  Initial Registration
  Certificate Renewal, Update, and Routine Re-key
  Re-key After Revocation
  Revocation Request
- Operational Requirements (Section 4)
  Application for a Certificate
  Certificate Issuance
  Certificate Acceptance
  Certificate Suspension and Revocation
  Security Audit Procedures

Records Archival
Key Changeover
Compromise and Disaster Recovery
CA Termination

- Physical, Procedural & Personnel Security (Section 5)

  Physical Controls
  Procedural Controls
  Personnel Controls
- Technical Security Controls (Section 6)

  Key Pair Generation & Installation
  Private Key Protection
  Other Aspects of Key Pair Management
  Activation Data
  Computer Security Controls
  Life-cycle Technical Controls
  Network Security Controls
  Cryptographic Module Engineering Controls
- Certificate & CRL Profiles (Section 7)

  Certificate Profile
  ARL/CRL Profile
- Specification Administration (Section 8)

  Specification Change Procedures
  Publication and Notification Procedures
  CPS Approval Procedures

2.7.5 Actions Taken as a Result of Deficiency

There are three possible actions to take when a deficiency has been identified:

- Continue to operate as usual
- Continue to operate but at a lower assurance level
- Suspend operation

If a deficiency is identified, the GPO PA will determine which of the following actions to take.

- If continuing operation, as usual or lower assurance level, the GPO PA and OA are responsible for ensuring that corrective actions are taken within 30 days. At that time, or earlier if agreed by the GPO PA and Compliance Auditor, the compliance audit team will re-audit the GPO-SCA in the areas of deficiencies. If, upon re-audit, corrective actions have not been taken, the GPO PA will determine if more severe action is required.
- If operation is suspended the GPO PA and OA are responsible for reporting the status of corrective action to the Compliance Auditors on a weekly basis. The GPO PA and Compliance Auditor together will determine when re-audit is to occur. If the deficiencies are deemed to have been corrected upon re-audit, the GPO-SCA will resume service.

2.7.6 Communications of Results

The compliance auditor will communicate results of all compliance audits to the PA through a Compliance Audit Report. The report will contain a summary table of topics covered, areas in which the GPO-SCA was found to be non-compliant and a brief description of the problems for each area of non-compliance. The report will also contain the detailed results of the compliance audit for all topics covered, including the topics in which the GPO-SCA passed and the topics in which the GPO-SCA failed.

Notification of compliance audit failure, the topics of failure and, reasons for failure will be provided immediately, upon the conclusion of the compliance audit, in a written report to the GPO-SCA OA and the GPO PA.

2.8 CONFIDENTIALITY

GPO-SCA information not requiring protection may be made publicly available, according to the stipulations of this CPS in the sub-sections below.

2.8.1 Types of Information to be Kept Confidential

Each Subscriber's private signing key is confidential to that Subscriber. The CA and RA are not provided any access to those keys.

Information held in audit logs is considered confidential to the GPO-SCA and is not released to external parties, unless required by law.

Personal information held by the RA, other than that which is explicitly published as part of a certificate, CRL, CP or this CPS is considered confidential to the GPO PKI and is not released unless required by law.

Generally, the results of annual compliance audits are kept confidential, with exceptions as outlined in this CPS.

The CPS itself is considered sensitive. The CPS will only be available for internal use by the GPO-SCA OA and GPO PA.

Operational details of the GPO-SCA, including physical and logical maps, connection diagrams, security measures, software used, disaster recovery plans and personnel utilization are considered sensitive and will be made available only to the GPO-SCA OA, Auditors, and others where approved by the GPO PA.

Information in transit between the RA and the GPO-SCA is automatically encrypted by the GPO-SCA and RA components to provide data confidentiality. Information stored on the RA workstation or GPO-SCA server is protected by password. The RA keeps paper information (e.g., registration forms) in a locked container when the RA is not present.

2.8.2 Types of Information Not Considered Confidential

Information included in certificates and CRLs issued by the GPO-SCA are not considered confidential.

Information in the CP supported by the GPO-SCA is not considered confidential.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

When the GPO-SCA revokes a certificate, a revocation reason is included in the CRL entry for the revoked certificate. The following table identifies the revocation reasons and the associated definitions.

Revocation Reason	Definition
Superseded	The certificate has been replaced but there is no suspicion of compromise.
Key Compromise	The private key corresponding to the public key in the certificate has been compromised or is suspected to be compromised.
Affiliation Change	Some information on the subject of the certificate has changed, but there is no suspicion of compromise.
Cessation of Operation	The certificate is no longer needed for its original purpose, but there is no suspicion of compromise.
Unspecified	None of the other four revocation reasons apply as to why the certificate was revoked.

This revocation reason code is not considered confidential and can be shared with the general public.

2.8.4 Release to Law Enforcement Officials

The GPO PA accepts all requests for information release to law enforcement officials and, working with the GPO General Counsel, will determine the applicability of compliance with the request.

The GPO PA keeps copies, either paper or electronic, of each request for information release to law enforcement officials.

2.8.5 Release as Part of Civil Discovery

The GPO PA accepts all requests for information release as part of civil discovery and, working with the GPO General Counsel, will determine the applicability of compliance with the request.

The GPO PA keeps copies, either paper or electronic, of each request for information release to law enforcement officials.

2.8.6 Disclosure Upon Owner's Request

The RA accepts digitally signed confidential information disclosure requests from Subscribers. If the signature is valid and the request is for information pertaining to the Subscriber, the RA will provide the requested information in a suitable format.

2.8.7 Other Information Release Circumstances

Except for audit log information, the GPO-SCA OA will not disclose any confidential information to a third party. Audit log information is only released to the authorized Auditor, upon written notification from the GPO PA.

All other requests for information will be forwarded to the GPO PA and the GPO General Counsel for a decision on release in accordance with the CP.

2.9 INTELLECTUAL PROPERTY RIGHTS

Certificates and CRLs issued by the GPO-SCA are the property of the GPO-SCA.

This CPS is the property of the GPO-SCA.

The Distinguished Names (DNs) used to represent End-Entities within the GPO-SCA domain in the directory and in certificates issued to End-Entities within that domain are the property of GPO.

With respect to licensed applications, this CPS does not modify ownership of licensed applications or licensing agreements for such applications.

3. IDENTIFICATION AND AUTHENTICATION

This section contains the practices to be followed in identifying and authenticating the personnel who are responsible for the operation and maintenance of the GPO-SCA. Additional practices are defined for identification and authentication of the subscribers.

3.1 INITIAL REGISTRATION

3.1.1 Types of Names

The GPO-SCA uses the X.500 Distinguished Names (DN) for all Subscribers. The DN may consist of naming elements C, O, OU and CN. The Naming Authority approved DN structures are as follows:

- For human Subscribers filling Trusted Roles:

  CN = [Subscriber first and last name, and *optionally*, a serial number] - The value of the serial number ***can*** be generated automatically to ensure uniqueness across all commonNames within a given directory path.
  OU = [CA Common Name]
  OU = [Administrators]
  OU = [Government Printing Office]
  O = [U.S. Government]
  C = [US]
  Example: "**cn=John Smith + *serialNumber=A123456*, ou=SCA, ou=Administrators, ou=Government Printing Office, o=U.S. Government, c=US**"
- For GPO human Subscribers:

  CN = [Subscriber first and last name, and *optionally*, a serial number] - The value of the serial number ***can*** be generated automatically to ensure uniqueness across all commonNames within a given directory path.
  OU = [People]
  OU = [Users]
  OU = [Government Printing Office]
  O = [U.S. Government]
  C = [US]
  Example: "**cn=John Smith + *serialNumber=A123456*, ou=People, ou=Users, ou=Government Printing Office, o=U.S. Government, c=US**"
- For Other Agency human Subscribers:

  CN = [Subscriber first and last name, and *optionally*, a serial number] - The value of the serial number ***can*** be generated automatically to ensure uniqueness across all commonNames within a given directory path.
  OU = [People]
  OU = [*OrgIdentifier*] – The value of the *OrgIdentifier* is going to be equal to the Other Agency name.
  OU = [Other Agencies]
  OU = [Government Printing Office]
  O = [U.S. Government]
  C = [US]
  Example: "**cn=John Smith + *serialNumber=A123456*, ou=People, ou=*AgencyName*, ou=Other Agencies, ou=Government Printing Office, o=U.S. Government, c=US**"
- For External human Subscribers:

  CN = [Subscriber first and last name, and *optionally*, a serial number] - The value of the serial number

can be generated automatically to ensure uniqueness across all commonNames within a given directory path.
OU = [People]
OU = [External]
OU = [Government Printing Office]
O = [U.S. Government]
C = [US]
Example: "**cn=John Smith + *serialNumber=A123456*, ou=People, ou=External, ou=Government Printing Office, o=U.S. Government, c=US**"

- For device component and server Subscribers:

  CN = [device name and model number and the device serial number OR application name, and optionally, the application module number]
  OU = [Devices]
  Followed by the directory branch that the device is associated with (see human subscriber examples with "People" replaced by "Devices"
  Example: "**cn=Cisco 12000 + *serialNumber=12XMZ4532*, ou=Devices, ou=Users, ou=Government Printing Office, o=U.S. Government, c=US**"
  Example: "**cn=Web Server Application + *serialNumber=Module 1*, ou=Devices, ou=Users, ou=Government Printing Office, o=U.S. Government, c=US**"

Certificates for human subscribers may contain a subscriber alternate name form in the subjectAltName field. The subscriber alternate name will be the rfc822 e-mail address. For organization, device component and server Subscriber certificates, the subjectAltName field will be populated with the rfc822 e-mail address of the human sponsor.

CRL distribution points are named with the commonName attribute with a value generated by the CA application and are named subordinate to the GPO-SCA.

3.1.2 Need for Names to be Meaningful

The value of the commonName attribute used in naming a SCA Subscriber is the Subscriber's first and last names.

3.1.3 Rules for Interpreting Various Name Forms

Distinguished names (DNs) and their component Relative Distinguished Names (RDNs) are to be interpreted in accordance with X.500 standards.

3.1.4 Uniqueness of Names

Names are unambiguously defined. The directory will be managed in such a way as to ensure that no two individuals are assigned the same DN, and therefore the same electronic identity.

3.1.5 Name Claim Dispute Resolution Procedure

The PA is ultimately responsible for resolution of any name claim disputes within the GPO PKI. However, because the commonName attribute is considered unique within the GPO PKI repository, such naming conflicts are expected to be rare.

3.1.6 Recognition, Authentication, and Role of Trademarks

The RA will not knowingly assign names that contain trademarks. The RA need not seek evidence of trademark registrations nor in any other way enforce trademark rights.

3.1.7 Method to Prove Possession of Private Key

Public key certificates bind a public key to the identity of the individual to assure Relying Parties that signing performed by the private key was done by the individual whose public key appears on the certificate, and decryption using the private key can only be performed by the individual whose public key appears on the certificate. This requires that an individual safeguard their private key and any activation data used to access that key.

The CA requires proof of possession of the private key before creating and signing a certificate containing the associated public key. Proof of possession of a private key is handled automatically by CA to Subscriber messages protected by PKIX-Certificate Management Protocol (CMP).

For the Subscriber's signature private key, a PKIX-CMP operation initiated by the Subscriber is digitally signed using the signature private key itself.

For the Subscriber's decryption private key, the GPO-SCA generates both public and private keys so no proof of possession is required.

3.1.8 Authentication of Organization Identity

The GPO-SCA will not be issuing organization certificates, except possibly to other subordinate CAs. The certificates issued by the GPO-SCA to subordinate CAs will be issued according to the requirements defined in the GPO CP and this CPS. All certificate requests for subordinate CAs will include identity information of the requesting representative which will be forwarded to the GPO PA for approval.

A signed MOA provides the organization identity authentication information.

3.1.9 Authentication of Individual Identity

There are different classifications of Subscribers and the initial registration process differs accordingly; however, all Subscribers are responsible for providing identity-proofing credentials as part of the initial registration process. The GPO-SCA issues Medium Assurance Certificates and the GPO CP requires in-person proofing for all Medium Assurance Certificates. The acceptable identification documentation required by Subscribers is one Federal picture ID or two Non-Federal IDs, one of which must be a Government issued picture ID (i.e. State issued Drivers License or State issued Picture ID Card). The CA administrators shall check to ensure that the certificate registration information supplied by the subscriber matches the identification credentials supplied for in-person proofing, and that no errors are contained in the certificate registration information supplied by the subscriber.

The following sections describe the initial registration processes for each of the classifications of Subscribers.

3.1.9.1 Entrust Master Users

All personnel holding Trusted Roles must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and present, in person, two pieces of identification credentials, a GPO issued GPO Employee badge or GPO issued GPO Contractor badge and another government issued photo ID (e.g. a Driver's license). The authentication is documented by a signed declaration from the PA or OAA that they personally verified the identity of the

Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification.

3.1.9.2 Entrust Officers

All personnel holding Trusted Roles must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and present, in person, two pieces of identification credentials, a GPO issued GPO Employee badge or GPO issued GPO Contractor badge and another government issued photo ID (e.g. a Driver's license). The authentication is documented by a signed declaration from two existing trusted users, a Master User and an existing Security Officer or two existing Security Officers that they personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification.

The initial Security Officer account, known as the First Officer, is created during the initial CA configuration. Two Master Users are responsible for authenticating the First Officer and verifying that the individual filling the role of First Officer properly completes the Trusted Role Subscriber Agreement and Registration Form. All subsequent Security Officers require authentication from at least two existing Security Officers, or one Security Officer and one Master User.

3.1.9.3 Entrust Administrators

To obtain their initial certificates, Administrators will enroll in person with two Security Officers. Administrators must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and provide two pieces of identification credentials, a GPO issued GPO Employee badge or GPO issued GPO Contractor badge and another government issued photo ID (e.g. a Driver's license). The authentication is documented by a signed declaration by the Security Officers that they personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification.

3.1.9.4 GPO Registration Authorities

GPO RAs can also be Entrust Administrators but are not necessarily Entrust Administrators. GPO RAs will enroll in person with an Entrust Administrator or GPO RA. RAs must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and provide identification credentials, a GPO Employee picture ID. The GPO RA's employment by GPO shall be verified by the GPO Entrust Administrator or GPO RA, using official GPO records to accomplish this verification. The authentication is documented by a signed declaration by the Entrust Administrator or GPO RA that they personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification. A biometric of the GPO RA (either a photograph or a fingerprint) shall be on file using official GPO records and available at all times to the RA or CA, or be captured and maintained on file by the RA or the CA.

3.1.9.5 Entity Registration Authorities

Entity RAs are part of an entity that the GPO-CA provides certificates to. An entity is any organization that GPO can provide services for, though typically these are federal government agencies from any of the three branches of federal government. Entity RAs can only act as RA

for their entity. All Entity RAs will be registered by an GPO Entrust Administrator in person. RAs must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and provide identification credentials, a Federal picture ID or two forms of ID at least one of which is a government issued photo ID (e.g. a Driver's license). The Entity RAs employment by the entity shall be verified by the RA, using official agency/entity records to accomplish this verification. The authentication is documented by a signed declaration by the GPO Entrust Administrator that they personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID, and the date and time of the verification. A biometric of the Entity RA (either a photograph or a fingerprint) shall be on file using official agency records (typically the photograph of the individual on the entity's ID badge for that individual) and available at any time to the GPO RA or CA, or captured and maintained on file by the GPO RA or the CA.

An Entity RA can only administer Subscribers in their respective Entity. Entity RA personnel must follow all aspects of this CPS and CPS RA procedures when administering certificate services (including certificate issuance, revocation and key recovery) for their entity's Subscribers. Entity RA's shall be required to utilize certificates stored on hardware tokens (just as GPO RA's are required to do), and shall follow all aspects of this CPS for RA operations. The hardware tokens shall be supplied by the GPO RA during Entity RA enrollment.

3.1.9.6 All Other Human Subscribers

To obtain their initial digital certificates, Subscribers will enroll in person with an RA or TA. Subscribers must complete and sign a Subscriber Agreement and a Registration Form signed by the Subscriber's supervisor and provide identification credentials, one Federal picture ID, or two other forms of ID at least one of which is a government issued photo ID (e.g. a State issued Driver's license). The Subscriber's employment by a federal agency shall be verified by the RA or TA, using official agency records to accomplish this verification. The authentication is documented by a signed declaration by the RA or TA that it personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification. A biometric of the Subscriber (either a photograph or a fingerprint) shall be on file using official agency records and available at all times to the RA or CA, or captured and maintained on file by the RA or the CA.

Subscribers will use either hardware or software cryptographic module validated to at least FIPS 140 Level 1 for generating and storing their cryptographic credentials.

3.1.10 Authentication of Component and Server Identities

Applications for a component or server certificate are made by an authorized human sponsor to whom the component or server's signature is attributable for the purposes of accountability and responsibility.

Identification and authentication of the human sponsor follows Section 3.1.9 as if the sponsor were applying for a certificate on their own behalf. In addition, the RA or TA will verify the authority of the sponsor to receive certificates for that component or server.

3.2 ROUTINE RE-KEY

Subscribers of the GPO-SCA shall have their affiliation with GPO reviewed periodically as stipulated in the GPO CP, commencing from the Subscriber's application submission date. Should a Subscriber no longer be eligible for a GPO-SCA certificate, the Subscriber's account will be deactivated and the Subscriber's existing certificates will be revoked.

3.2.1 Certificate Re-Key

3.2.1.1 SCA Trusted Role Certificate Re-Key

The SCA Trusted Role keys are automatically updated prior to expiration of the current key pairs.

3.2.1.2 SCA Subscriber Certificate Re-Key

The SCA Subscriber keys are automatically updated prior to expiration of the current key pairs.

3.2.2 Certificate Renewal

The SCA does not support certificate renewal. If a Subscriber requires certificate renewal for any reason, the Subscriber will require a certificate re-key.

3.2.3 Certificate Update

The SCA will support certificate update for name change. When a Subscriber's name changes (i.e. due to marriage) the name data contained in a certificate requires changing. A DN change will be performed creating a new set of certificates issued with the new name and new keys after the Subscriber provides, in person, proof of name change.

3.3 RE-KEY AFTER REVOCATION

All GPO-SCA Subscribers must repeat the initial certificate registration and request process in order to obtain a new certificate after a revocation.

3.4 REVOCATION REQUEST

Revocation requests can be made by a Subscriber or another person authorized to act on behalf of the Subscriber (e.g., supervisor, HR department, etc.). All certificate revocation requests are communicated to an RA via secure means, either electronically or in person.

An RA may process a revocation request from a TA, based on an email revocation request that has been digitally signed by the TA.

An RA may process a revocation request from a Subscriber, based on an email revocation request that has been digitally signed by the Subscriber.

An RA may process a revocation request based on a digitally signed email from an individual authorized to request revocation on behalf of the Subscriber (e.g. the Subscriber's supervisor, HR representative, etc.). In this case, the RA will verify the authority of the requestor to submit the revocation request by validating the digital signature against an authoritative source.

An RA may process an in-person revocation request from a Subscriber, following authentication as outlined in Section 3.1.9.

3.5 CERTIFICATE RE-KEY, RECOVERY AND UPDATE

3.5.1 Certificate Re-Key

The GPO-SCA Subscriber keys are setup to be automatically re-keyed prior to expiration of the current key pair, based on possession of the non-expired private key. PKIX-CMP protected messages invoked by the GPO-SCA application update the Subscriber's keys transparently.

Re-authentication of the Subscriber's identity as defined in Section 3.1.9 of this CPS will be repeated periodically as specified in the GPO CP.

3.5.2 Certificate Recovery

3.5.2.1 Recovery of Security Officers

When a Security Officer (applicant) needs certificate recovery, he/she must complete and sign a Certificate Recovery Request Form and present himself or herself in person to another Security Officer. The Security Officer performing the recovery will:

- Complete identification and authentication, as defined in Section 3.1.9
- Setup the applicant for certificate recovery
- Provide the shared secret data to the applicant
- Have the applicant create their profile
- Sign the Certificate Recovery Request Form indicating that they witnessed the applicant performing certificate recovery

The Certificate Recovery Request Form will be stored by the OA and will be made available during all compliance audits.

3.5.2.2 Recovery of Administrators

When an Entrust Administrator (applicant) needs certificate recovery, he/she must complete and sign a Certificate Recovery Request Form and present himself or herself in person to a Security Officer or another Administrator for recovery:

- Complete identification and authentication, as defined in Section 3.1.9
- Setup the applicant for certificate recovery
- Provide the shared secret data to the applicant
- Have the applicant create their profile
- Sign the Certificate Recovery Request Form indicating that they witnessed the applicant performing certificate recovery

The Certificate Recovery Request Form will be stored by the OA and will be made available during all compliance audits.

3.5.2.3 Recovery of Registration Authorities

An RA recovery is completed by:

- Complete a Recovery Request
- Identify and Authenticate RA to be recovered

- Setup RA for recovery
- Generate reference number and authorization code
- Have the RA recover their profile

Auditable information on all Certificate Recovery Requests will be stored by the OA and will be made available during all compliance audits.

3.5.2.4 Recovery of and Subscribers

A Subscriber recovery is completed by:

- Complete a Recovery Request
- Identify and Authenticate Subscriber to be recovered
- Setup Subscriber for recovery
- Generate reference number and authorization code
- Have the Subscriber recover their profile

Auditable information on all Certificate Recovery Requests will be stored by the OA and will be made available during all compliance audits.

3.5.3 Certificate Update

The GPO-SCA will support certificate update for name change. The applicant for certificate update must present himself or herself in person and provide proof of name change. After proof of name change a Distinguished Name (DN) change can be performed on the CA, this will issue a new certificate with the new name for the applicant.

4. OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Cross-Certification Certificate Application

The GPO-SCA does not issue cross-certificates, and as such, does not process cross-certification certificate applications.

4.1.2 Subscriber Certificate Application

4.1.2.1 GPO-SCA Subscribers Filling Trusted Roles

GPO-SCA Subscribers filling Trusted Roles are nominated by the GPO-SCA OA to the GPO PA in a signed memorandum - electronic transmission with digital signature is permitted. The GPO PA authorizes the GPO-SCA OA to add the nominee to the CA Administrators group in the directory and to approve a certificate for that nominee.

Prior to certificate issuance, GPO-SCA Subscribers filling Trusted Roles perform the identification and authentication as specified in Section 3.1.9. Upon successful completion of the identification and authentication procedures, the Trusted Role Subscriber is given the shared secret data required for certificate generation, for RAs a hardware token validated to at least FIPS 140 Level 2 is required. The Subscriber indicates acceptance of the token and shared secret data in a signed acceptance document – requires handwritten signature.

The GPO-SCA OA will keep a copy of all GPO-SCA Trusted Role Subscriber Registration Request.

4.1.2.2 All Other Human Subscribers

Prior to certificate issuance, GPO-SCA Subscriber applicants will present themselves to an RA or TA and provide the required identification, as specified in Section 3.1.9.

The GPO-SCA RA creates the Subscriber's PKI account with the CA. The CA returns shared secret data consisting of a reference number and an authorization code. The RA then provides the reference number to the Subscriber. The authorization code is sent, unencrypted, to the Subscriber's organization e-mail address.

The Subscriber completes the certificate issuance process.

If the Subscriber does not complete the certificate issuance process within the allowable 30-day window, the reference number and authorization code will automatically become invalid and the Subscriber will have to repeat the initial application.

The GPO-SCA OA will keep a copy of all GPO-SCA Subscriber certificate applications.

4.1.2.3 Component and Server Subscribers

The human sponsor is responsible for contacting the GPO-SCA RA to request a component or server certificate. The GPO-SCA RA will authenticate the sponsor in accordance with Section 3.1.10.

Upon successful completion of the identification and authentication procedures, the GPO-SCA RA will access the CA registration application to create the component or server Subscriber's

PKI account with the CA. The CA creates shared secret data consisting of a reference number and an authorization code.

The sponsor uses the reference number and the authorization code complete certificate creation.

The GPO-SCA OA will keep a copy of all component or server certificate applications.

4.1.3 Delivery of Public Key for Certificate Issuance

Subscriber's encryption public keys are generated by the GPO-SCA, and thus require no delivery mechanism.

Subscriber signature verification public keys are generated on the Subscriber's token, and delivered to the GPO-SCA using the PKIX-CMP protocol to provide both integrity and privacy.

4.2 CERTIFICATE ISSUANCE

The CA binds the identity information in the certificate application with the public keys during the certificate issuance process.

A Subscriber, using their newly generated signing key, digitally signs the certificate request. Upon receipt of a valid request, the GPO-SCA automatically generates an encryption key pair and issues a signature verification public key certificate and an encryption public key certificate for that Subscriber. The Subscriber certificates and the decryption private key, as well as the GPO-SCA's verification certificate and the GPO PCA verification certificate, are provided to the Subscriber by the GPO-SCA using the PKIX-CMP protocol to provide both integrity and privacy, which also includes a specific message via the user interface to the Subscriber indicating success or failure of certificate issuance.

For certificates issued to subscribers on hardware tokens (smartcards, for example), an authorized PKI Trusted Role staff member will issue the token to the subscriber. The OA and Trusted Role staff shall securely maintain the stock of hardware tokens prior to issuance. The token serial number of any token issued to a subscriber shall be recorded on the certificate application paperwork. Tokens may be re-used for other subscribers once the key destruction process, using the vendor supplied initialization and key zeroization software, has been implemented by an authorized Trusted Role staff member. Tokens associated with a key compromise event are not to be re-used.

4.2.1 GPO-SCA Subscribers Filling Trusted Roles

The Trusted Role Subscriber uses the RA workstation to enter the reference number and authorization code provided during certificate application to complete the private key generation and certificate issuance process.

4.2.2 All Other Human Subscribers

The Subscriber uses the reference number and authorization code to complete the certificate issuance.

4.2.3 Component and Server Subscribers

Upon the completion of the certificate application, the human sponsor for the component or server Subscriber must generate the certificate request according to the component or server manufacturer's directions.

The human sponsor then submits the certificate request to the appropriate CA interface (i.e. Enrollment Server for VPN, Enrollment Server for Web, etc.) and authenticates the request with the reference number and authorization code provided during certificate application.

The CA interface then completes the certificate issuance process.

In some cases, PKIX-CMP may be supplemented by the use of other procedures such as Public Key Crypto Standard 10 (PKCS #10), or Cisco's Simple Certificate Enrollment Protocol (SCEP).

4.2.4 Delivery of Subscriber's Private Key to Subscriber

Subscribers generate their own private signature key, and as such, there is no need for delivery of the private signature key.

Subscriber's private decryption keys are delivered to the Subscriber from the GPO-SCA using the PKIX-CMP protocol to provide both integrity and privacy.

4.2.5 CA Public Key Delivery and Use

The GPO-SCA's verification certificate is provided to all Subscribers during the certificate issuance phase.

Relying Parties must also be granted access to the GPO-SCA's verification certificate, as well as the GPO-PCA's verification certificate in order to establish and verify certification trust paths. In order to distribute the GPO-SCA verification certificate, the GPO-SCA publishes its verification certificate in the GPO PKI Repository.

4.3 CERTIFICATE ACCEPTANCE

All Subscribers submit a signed PKI Subscriber Agreement, which includes a Registration Form and the Subscriber Obligations. The Subscriber's signature on the PKI Subscriber Agreement will be deemed as the acceptance of the certificate and acceptance of the obligations and responsibilities as defined in the Subscriber Agreement.

The successful completion of the Certificate Issuance process constitutes the technical acceptance of the certificates.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

The GPO-SCA does not support suspension, and as such, the following sub-sections pertain strictly to certificate revocation.

4.4.1 Revocation

4.4.1.1 Circumstances for Revocation

Certificates will be revoked when any of the following circumstances occur:

- Subscriber's private key is lost, stolen, suspected of compromise, or compromised

- Subscriber is suspected of fraud or other adverse behavior
- Subscriber leaves or is no longer affiliated with GPO or the sponsoring Agency
- Subscriber's identifying information contained in the certificate is no longer valid
- Subscriber violates the Subscriber Agreement
- Subscriber or other authorized party asks for Subscriber's certificate to be revoked

4.4.1.2 Revocation Requesters

The GPO PA or GPO-SCA OA can request revocation of any Subscriber certificate issued by the GPO-SCA. A written notice and brief explanation shall subsequently be provided to the affected Subscriber.

RAs can request revocation of a Subscriber's certificate. A Subscriber can always request revocation of a certificate in which they are listed as the certificate subject. A Subscriber's authorized Agency management official may request revocation.

4.4.1.3 Procedure for Revocation Request

When any of the circumstances for certificate revocation occur, the OA receives the revocation request and must process the request within the period specified in the GPO CP.

The all revocation requests will review to ensure they are legitimate and will then revoke the certificate, as follows:

- Authenticate the person requesting revocation
- Verify the person requesting revocation is authorized to request revocation of the certificate in question
- Authenticate revocation request
- Revoke the certificate, specifying revocation reason
- Ensure the revocation request is kept by the OA

For GPO-SCA Subscribers using hardware tokens, the hardware token will be surrendered to the GPO-SCA OA and the GPO-SCA OA will zeroize the token using the token vendor provided utility.

4.4.1.4 Certificate Revocation

Revocation shall take effect upon the publication of the CRL (identifying the reason for the revocation, which may include loss, compromise, or termination of employment). Information about a revoked certificate shall remain on the CRL even after the certificate expires.

4.4.1.5 Revocation Request Grace Period

As stipulated in the GPO CP.

4.4.2 Suspension

The GPO CP does not permit suspension.

4.4.3 Certificate Revocation Lists

Certificates that have been revoked shall **not** be removed from the CRL, they shall remain on the CRL even after the certificate expires.

4.4.3.1 Revocation List Issuance Frequency

The GPO-SCA server shall issue CARL/CRLs at least once every 18 hours. Additional CRLs will be issued and published to the directory upon certificate revocation.

4.4.3.2 CRL/CARL Checking Requirements

Each certificate issued by the GPO-SCA includes the full DN of the CRL Distribution Point to be checked during the verification of the certificate. Relying parties, when working in an online mode, shall check the current CRL, identified by the DN in the certificate's cRLDistributionPoints extension field, along with any other CRLs required in certificate chain processing prior to trusting the certificate.

When working in an offline mode, relying parties may not able to perform full CRL checking. When relying parties do not perform CRL checking, they accept the certificates at their own risk.

4.4.4 On-Line Revocation Status Checking

The GPO-SCA does support on-line revocation/status checking using the OCSP protocol.

A verification (signing) key issued by the GPO SCA is used for the purpose of signing OCSP response messages.

Error messages in response to certificate status requests are not signed, as provided for in the PKIX OCSP standard, RFC 2560.

4.4.5 Other Forms of Revocation Checking

No alternate methods of revocation advertisements are used for Subscriber certificates.

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements

There are no other forms of revocation advertisement used.

4.4.7 Special Requirements Related to Key Compromise

CARLs are used to advertise CA private key compromise or loss.

4.5 SECURITY AUDIT PROCEDURES

All security events on the CA's system are automatically recorded in audit log files. Such files are securely archived in accordance with the GPO CP and this CPS as well as other applicable GPO information systems security policies.

As specified in the GPO CP, there are other auditable events that are not captured in electronic audit logs. These events, such as physical access events, are manually recorded in paper logs.

The GPO-SCA OA is responsible for ensuring that all manual audit log events, as defined by the GPO PA and the compliance auditor are properly logged and the logs maintained as required.

4.5.1 Types of Events Recorded

The following table identifies additional audit events that are recorded:

Auditable Event	Method	Location
SECURITY AUDIT		
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	Manually	CP or CPS change control
Any attempt to delete or modify the Audit logs	Automatically	OS logs
IDENTIFICATION AND AUTHENTICATION		
Successful and unsuccessful attempts to assume a role	Automatically	CA logs
Change in the value of maximum authentication attempts	Automatically	CA logs
Maximum number of unsuccessful authentication attempts during user login	Automatically	CA logs
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	Automatically	CA logs
An Administrator changes the type of authenticator, e.g., from password to biometrics	Automatically	CA logs
KEY GENERATION		
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Automatically	CA logs
PRIVATE KEY LOAD AND STORAGE		
The loading of Component private keys	Automatically	CA logs
All access to certificate subject private keys retained within the CA for key recovery purposes	Automatically	CA logs
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
All changes to the trusted public keys, including additions and deletions	Automatically	CA, OS logs[1]

1 Auditing of changes to trusted public keys can take place in various locations. These changes will be audited by the server OS or CA application (if performed through the CA).

Auditable Event	Method	Location
PRIVATE KEY EXPORT		
The export of private keys (keys used for a single session or message are excluded)	Automatically	CA logs
CERTIFICATE REGISTRATION		
All certificate requests	Manually	RA logs
CERTIFICATE REVOCATION		
All certificate revocation requests	Manually	RA logs
CERTIFICATE STATUS CHANGE APPROVAL		
The approval or rejection of a certificate status change request	Manually	RA logs
CA CONFIGURATION		
Any security-relevant changes to the configuration of the CA	Automatically	CA logs
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted	Automatically	CA logs
The access control privileges of a user account or a role are modified	Automatically	CA logs
CERTIFICATE PROFILE MANAGEMENT		
All changes to the certificate profile	Automatically	CA logs
REVOCATION PROFILE MANAGEMENT		
All changes to the revocation profile	Automatically	CA logs
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the certificate revocation list profile	Automatically	CA logs
MISCELLANEOUS		
Installation of the Operating System	Automatically	OS logs
Installation of the CA	Automatically	CA, OS logs
Installing hardware cryptographic modules	Automatically	CA logs
Removing hardware cryptographic modules	Automatically	CA logs
Destruction of cryptographic modules	Automatically	CA logs
System Startup	Automatically	OS logs
Logon Attempts to CA applications	Automatically	CA logs
Receipt of Hardware / Software	Manually	OA logs

Auditable Event	Method	Location
Attempts to set passwords	Automatically	OS logs
Attempts to modify passwords	Automatically	OS logs
Backing up CA internal database	Automatically	CA logs
Restoring CA internal database	Automatically	CA logs
File manipulation (e.g., creation, renaming, moving)	Automatically	OS logs
Posting of any material to a repository	Automatically	CA, OS and Dir logs
Access to CA internal database	Automatically	CA logs
All certificate compromise notification requests	Manually	RA logs
Loading tokens with certificates	Automatically	CA logs
Shipment of Tokens	Manually	RA logs
Zeroizing tokens	Manually	RA logs
Re-key of the CA	Automatically	CA logs
Configuration changes to the CA server involving:		
Hardware	Manually	OA logs
Software	Manually	OA logs
Operating System	Manually	OA logs
Patches	Manually	OA logs
Security Profiles	Manually	OA logs
PHYSICAL ACCESS / SITE SECURITY		
Personnel Access to room housing CA	Manually	OA logs
Access to the CA server	Manually	OA logs
Known or suspected violations of physical security	Manually	OA logs
ANOMALIES		
Software Error conditions	Automatically	CA logs
Software check integrity failures	Automatically	CA logs
Receipt of improper messages	Automatically	CA, OS logs
Misrouted messages	Automatically	OS logs
Network attacks (suspected or confirmed)	Automatically	CA, OS logs
Equipment failure	Manually	OA logs
Electrical power outages	Manually	OA logs
Uninterruptible Power Supply (UPS) failure	Manually	OA logs
Obvious and significant network service or access failures	Manually	OA logs

Auditable Event	Method	Location
Violations of Certificate Policy	Manually	PA logs
Violations of Certification Practice Statement	Manually	OA logs
Resetting Operating System clock	Automatically	OS logs

4.5.2 Frequency of Processing Data

A Security Compliance Officer manually reviews the audit logs via the Entrust Security Manager Administration application, for policy violations or other significant events at least once per month.

The audit logs are made available during any compliance audits.

4.5.3 Retention Period for Security Audit Data

The audit log data is kept live on the CA or RA hardware and archived as specified in the GPO CP.

4.5.4 Protection of Security Audit Data

Current physical logs (e.g., visitor sign-in logs) will be kept in the CA equipment location rooms. Only authorized personnel will have access to the physical log and only authorized personnel will make entries in physical log or other paper audit records.

The CA audit log is stored in regular operating system flat files. Each audit log file consists of an audit header, which contains information about the audits in the file and list of events. A Message Authentication Code (MAC) is created for each of the audit events and the audit log header. Each audit log file has a different audit key used to generate the MAC. The Entrust master key for the GPO-SCA is used to encrypt the audit key; the encrypted audit key is stored in the audit header.

The audit log can be spread across many files. A new audit log file is created when the current audit log file reaches a preset size of 1 Mbytes or the Entrust master key is updated.

4.5.5 Security Audit Data Backup Procedures

The security audit data backup is archived by the OA Backup Operator on a weekly basis. All files including the latest audit log file are copied to magnetic tape, or some other secure media and stored in a secure archive facility.

4.5.6 Security Audit Collection System (Internal vs. External)

The CA audit system is internal to the Entrust Authority Security Manager software. The CA audit system is automatically invoked at CA system startup, and cease only at CA system shutdown. If it is determined that the automated CA audit system has failed and is not operational, CA operations shall be suspended until the audit system failure has been resolved. The GPO PA shall determine whether to resume operations after such an audit system failure.

4.5.7 Notification to Event-Causing Subject

The GPO CP imposes no requirement to notify a Subject that an event was audited.

4.5.8 Vulnerability Assessments

The GPO-SCA OA and the Compliance Auditor will be watchful for anomalies and attempts to violate the integrity of the system, including the equipment, its physical location, and its personnel. The OA will, as part of its regular security audit review, look for events such as repeated failed actions, requests for privileged information, attempted access of system files, unauthenticated responses, and continuity of security audit data.

Suspicious activity will be reported to the GPO PA.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Archived

The following table identifies the archive records that are retained:

Archive Records
CA accreditation (if applicable)
Certification Practice Statement
Contractual obligations
System and equipment configuration
Modifications and updates to system or configuration
Certificate requests
Revocation requests
Subscriber identity Authentication data
Documentation of receipt and acceptance of certificates
Documentation of receipt of tokens
All certificates issued or published
Record of CA Re-key
All information on ARLs and CRLs issued and/or published
All Audit Logs
Other data or applications to verify archive contents
Documentation required by compliance auditors
Certificate Policy

Archive Records
Other agreements concerning operations of the CA
Subscriber agreements
Subscriber encryption-decryption key pairs

4.6.2 Retention Period for Archive

Archive records are kept as specified in the GPO CP. Applications required to process the archive data will also be maintained for the archive retention period. The GPO-SCA OA is responsible for knowing where the archived material is, and for ensuring that it is not lost during reorganizations, physical organization moves, and so on.

Archive records that have been kept for 20 years are transferred to a GPO PA approved archive facility for indefinite storage.

4.6.3 Protection of Archive

When possible the archive data will be digitally signed by the GPO-SCA. This will provide an integrity check that can be used to verify that the data has not been modified.

Long-term archive data for the GPO-SCA will be recorded on read-only media and stored off-site in a fireproof safe/vault with locks. Short-term media will be stored in a location separate from the CA equipment. The archive media is protected by physical security in that it is retained in a restricted access location to which only the GPO PA and GPO-SCA OA have access. This location will adhere to the physical security practices defined in this CPS.

The archives will be labeled with the CA DN and the date.

A list of authorized individuals that have the permissions necessary to access and delete the on-line archive files will be maintained at the CA site, and all accesses will be recorded. These records will be made available to the auditors during compliance audits.

4.6.4 Archive Backup Procedures

Archive files are backed up along with the security audit logs.

Paper archives may be backed up to microfiche, or other long-term storage solution, as directed by the PA.

4.6.5 Requirements for Time-Stamping of Records

Time-stamping of records is accomplished via the CA system, using the CA system clock. The CA system clock is synchronized on a periodic basis with an authoritative time source, to ensure that the CA system clock is accurate.

4.6.6 Archive Collection System (Internal and External)

GPO-SCA archive data will be collected as part of the routine system backup procedures, along with directory shadowing, and explicit file copies of GPO-SCA files that do not reside in the underlying GPO-SCA database. Paper based CA records that are required for archive will be

copied or digitally scanned, and packaged by the Operational Authority for transmittal to the archive site. The Operational Authority shall verify that all required archive records are contained in packages that are transmitted and moved to the archive facility.

4.6.7 Procedures to Obtain and Verify Archive Information

The archive system automatically verifies the archive media immediately after archive creation.

The OA is responsible for ensuring that all request for archive information come from an authorized source. The archive condition is verified during every compliance audit.

4.7 CA KEY CHANGEOVER

The Subscriber certificates issued by the GPO-SCA are set up for automatic key roll-over. As such, the encryption and digital signature key pairs of the Subscriber are automatically updated prior to expiry. Following CA key changeover, the new CA key will be used to CRLs and certificates going forward.

4.8 COMPROMISE AND DISASTER RECOVERY

The PA and OA maintain a GPO PKI Contingency Plan, which is updated periodically (at least on an annual basis) or as major system changes dictate, to define how the PKI is restored to service in a reasonably timely manner in the event of a failure. The GPO PKI Contingency Plan shall define the acceptable system outage and recovery time periods.

In any key compromise situation, a report will be filed with the PA indicating the circumstances under which the compromise occurred. The PA will determine if a possible follow up investigation and potential action is required.

4.8.1 Computing Resources, Software, and /or Data are Corrupted

In the event of an inoperative SCA due to equipment damage, software or Operating System failure, or data corruption, where all copies of the CA signature keys are **not** destroyed, the following steps, at a minimum, are taken to recover a secure environment:

- The SCA infrastructure (hardware and software) will be re-built and/or restored from backup as necessary
- The SCA shall be reconstituted within 72 hours, in the event of a catastrophic failure
- The directory data, encryption certificates and CRLs/ARLs, are restored if the directory becomes unusable and must be restored from backup or if the directory is suspected to be corrupt.

4.8.2 CA Signature Keys are Revoked

In the event of an inoperative SCA, where all copies of the SCA signature keys are **not** destroyed, the following steps, at a minimum, are taken to recover a secure environment:

- The SCA infrastructure (hardware and software) will be re-built and/or restored from backup as necessary

- The directory data, encryption certificates and CRLs/ARLs, are restored if the directory becomes unusable and must be restored from backup or if the directory is suspected to be corrupt
- The Policy Authority shall be informed, as well as any entity Policy Authorities that are cross-certified with the GPO PCA or SCA, in the event that the CA cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL

4.8.3 CA Signature Keys are Compromised

In the event of the compromise of the SCA private key, the PA will be informed via secure communication from the OA. The PA will authorize and instruct the OA to revoke the certificates for the SCA (any CRL issued must be valid until 30 days after the last certificate issued by the SCA expires), install a new SCA, generate a new SCA certificate, and publish the new SCA certificate to the directory.

The OA will notify the Subscribers of the SCA of the key compromise via a secure communication. When available, every SCA Subscriber will be required to re-register in-person, to be moved to the new SCA, and install the new SCA certificate.

4.8.4 Secure Facility Impaired After a Natural or Other Type of Disaster

In the event of a disaster of the SCA when the SCA private key is not compromised and is available, the following steps, as a minimum, are taken to recover a secure environment:

- The SCA infrastructure (hardware and software) will be re-built at an alternate facility
  - The alternate facility is located at least 50 miles away from the primary SCA facility
  - The SCA infrastructure is built and on stand-by at the alternate facility
- The directory data, encryption certificates and CRLs/ARLs, are restored to the directory
- In the event that the disaster results in all copies of the CA keys being destroyed, the Policy Authority (PA) shall be notified at the earliest feasible time, and the PA shall take actions it deems appropriate

4.9 CA CESSATION OF SERVICES

In the event that the GPO-SCA ceases operation or is otherwise terminated:

- All Subscribers and Relying Parties must be promptly notified of the cessation
- All Subscribers will be notified of cessation using email communication, if email is available
- All certificates issued by the GPO-SCA shall be revoked no later than the time of cessation (any CRL issued must be valid until 30 days after the last certificate issued by the SCA expires)
- All current and archived GPO-SCA identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be sent to the GPO PA archive facility

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS FOR THE GPO-CA

The GPO-SCA equipment is labeled as being for authorized use only. GPO-SCA equipment is in a controlled facility. GPO-SCA cryptographic modules are protected against theft, loss, and unauthorized use.

5.1.1 Site Location and Construction

GPO-SCA equipment is located in facilities approved by GPO as being appropriate for storing sensitive material. The GPO-SCA OA will keep a copy of documentation approving the GPO-SCA site and will provide the documentation for inspection during compliance audits.

5.1.2 Physical Access

An integrated physical access control and intrusion detection system will restrict access to authorized personnel, detect unauthorized access, and provide for the audit of all entries to and exits from the controlled areas. Sensors monitor exit and entrance doors.

The Security Zone is designated as a two-person zone.

An access control policy is posted in the Operations zone and includes sign-in sheets for visitors. The policy requires all persons to wear an approved building pass and visitors to be escorted at all times within these high security zones.

Entrance to, and exit from, all controlled areas is monitored by closed circuit television (CCTV) and an appropriate system is used to record images or persons passing through the area. In addition, an appropriate camera and time-lapse recorder will record activity in the security zone. The camera is placed such that persons in the room are recorded, but such that keystrokes typed on the system console may not be recovered by image enhancement. Images/recordings are maintained for a minimum of 90 days. (Note: The requirement for video recording within the security zone shall be waived if it violates local employment or privacy regulations/legislation.)

CA facilities are checked by security personnel at least once per business day to ensure that the physical protection mechanisms are still operating and ensure that there has not been an attempt to gain unauthorized access to the CA area. Records of these checks (including the names of the individuals making the check, along with a date and time) will be provided to the auditor during every compliance audit.

Only trusted PKI personnel will be given the keys, access cards, or the combination numbers required to access the CA equipment rooms/zones (as noted above visitors must sign in and will be escorted at all times).

5.1.3 Power and Air Conditioning

All controlled access areas in the Security Zone shall be equipped with:

- An appropriately sized uninterruptible power supply sufficient to allow for the systems to complete current actions and shutdown without data loss, and for six (6) hours of uninterruptible power for the directory servers

- Heating, ventilation, and air conditioning appropriate for a commercial data processing facility
- Emergency lighting

These environmental controls shall conform to local standards and shall be appropriately secured to prevent unauthorized access and/or tampering with the equipment.

No liquid, gas, exhaust, etc. pipes shall traverse the controlled space other than those directly required for the area's HVAC system.

5.1.4 Water Exposures

The GPO-SCA equipment will be installed such that it is not in danger of exposure to water. Sprinklers used for fire control have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.

5.1.5 Fire Prevention and Protection

The GPO-SCA secure facility is fully wired for fire detection, alarm and suppression. Routine, frequent inspections of all systems are made to assure adequate operation.

5.1.6 Media Storage

All media is stored away from sources of heat, and away from obvious sources of water (e.g., away from water pipes) or other obvious hazards. Electromagnetic media (tapes, diskettes, etc.) are stored away from obvious sources of strong magnetic fields (audio speakers, monitors). Archived material is stored in a room or building separate from the GPO-SCA equipment until it is transferred to the approved archive storage facility.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed and are to be destroyed shall be destroyed in a process that renders the material unrecoverable.

5.1.8 Off-Site Backup

Full system backups, sufficient to recover from system failure, are to be accomplished not less than once per week. A full system backup shall be stored at an off-site location (separate from the CA equipment), with physical controls commensurate with the operational CA.

5.2 PROCEDURAL CONTROLS FOR THE GPO-CA

5.2.1 Trusted Roles

The GPO CP defines the following Trusted Roles:

- OA System Administrator
- OA Officer – Master User
- OA Officer – Security Officer
- OA Officer – Administrator
- OA Officer – Directory Administrator

- Security Compliance Auditor
- OA Backup Operator

The following table identifies the relation of the GPO Trusted Roles, and Entrust product roles:

GPO Role	Entrust Role
OA System Administrator	N/A
OA Officer – Master User	Master User
OA Officer – Security Officer	Security Officers (includes the First Officer)
OA Officer – Administrator	Administrator
OA Officer – Directory Administrator	Directory Administrator
Security Compliance Auditor	Auditor
OA Backup Operator	N/A

Each role is explained in following sections.

5.2.1.1 GPO OA System Administrator

The OA System Administrator is responsible for initially installing and configuring the GPO-SCA operating system and for performing ongoing system administration duties such as account management, access control management, system configuration management, database maintenance, software upgrades, and compromise reporting.

5.2.1.2 GPO OA Officer – Master Users

There are three Entrust Authority Master Users. Their Entrust Authority Master User passwords are documented and stored in a safe approved by the OA. The Master Users have authority to:

- Configuring certificate profiles or templates
- Generating and backing up CA keys
- Maintain Entrust Authority services (consisting of Administration Service and Key Management Service) plus the Entrust Authority database
- Recover the Entrust Administration service, in the event its profile becomes damaged
- Backup, re-encrypt and restore from backup as necessary, the Entrust Manager database

5.2.1.3 GPO OA Officer – Security Officers

The Entrust Security Officer created during the installation of the Entrust Authority is the *First Officer*. The First Officer, drawing from selected GPO personnel, creates additional Entrust Security Officers. The main role of an Entrust Security Officer is to set and administer the GPO-SCA's security policy as it applies to all Subscribers. Entrust Security Officers have the following privileges:

- Verifying the identity of Trusted Role Subscribers and accuracy of information included in certificates

- Set the security policy for the GPO-SCA, and alter it
- Add, delete and revoke other Entrust Security Officers, Entrust Administrators, and Directory Administrators
- Authorize sensitive operations, such as adding and deleting Security Officers and Administrators

The names of the Security Officers will be made available to the Compliance Auditor during each compliance audit.

5.2.1.4 GPO OA Officer – Administrators

For the GPO-SCA, the Entrust Administrators are responsible for:

- Verifying the identity of GPO-SCA Subscribers
- Securely communicating requests to and responses from the CA
- Executing revocation requests received from authorized sources

The names of the Registration Authorities will be made available to the Compliance Auditor during each compliance audit.

5.2.1.5 GPO OA Officer – Directory Administrators

The Directory Administrators are responsible for maintaining the certificate repository. The Directory Administrator can be an OA Officer – Security Officer or OA Officer – Administrator, but may **not** be an OA Officer – Master User.

5.2.1.6 GPO Security Compliance Auditor

The Security Compliance Auditor also known as the Security Compliance Officer (SCO) is responsible for reviewing, but not modifying audit logs, various reports, Security Policy and user properties. The Security Compliance Auditor is responsible for performing or overseeing internal compliance audits to ensure that CA is operating in accordance with its CPS

The names of the Security Compliance Auditor(s) will be made available to the Compliance Auditor during each compliance audit.

5.2.1.7 GPO OA Backup Operator

The OA Backup Operator is responsible for performing backups, duplicating backups, secure storage of backups, and restoring from backups.

5.2.1.8 Registration Authorities

For the GPO-SCA, the Registration Authorities are responsible for:

- Verifying the identity of GPO-SCA Subscribers
- Securely communicating requests to and responses from the CA
- Executing revocation requests received from authorized sources

The names of the Registration Authorities will be made available to the Compliance Auditor during each compliance audit.

A Local Registration Authority (LRA) or Trusted Agent may verify the identity of Subscribers during the registration process. LRAs are individuals appointed and/or recognized by the OA.

Trusted Agents are individuals such as Notary Publics, and may verify the Subscribers identity if the Subscriber is unable to complete identity verification with an RA or LRA.

5.2.2 Separation of Roles

Systems Administrators do not have access to the Security Manager Administration application.

Since GPO intends to have the GPO-SCA issue certificates as a service to other Entities, and allow them to have RAs, LRAs and TAs that administer the certificates issued to Entity Subscribers, the RA, LRA and TA privileges will be determined based on the agreement with the Entity.

The following table identifies the GPO Trusted Roles and the privileges assigned to each role within the Entrust CA:

Privilege	**Trusted Roles**			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Administrator**	**Security Compliance Auditor/Officer**
Default User Policy certificate	N/A	Security Officer Policy	Administrator Policy	Administrator Policy
Audit Logs				
View own logs		X	X	X
View all logs		X	X	X
Bulk & Report				
Process bulk files		X	X	
Create reports		X	X	X
Certificates				
Admin all categories		X	X	X
Admin selected categories				
Admin all types		X	X	X
Certification Authority				
Stop, Start and Maintain CA Services	X			
Recover Admin Service	X			
Backup and Restore CA databases				
View CA certificates		X	X	X

Privilege	Trusted Roles			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Administrator**	**Security Compliance Auditor/Officer**
Update CA signing keys		X		
Revoke CA keys		X		
View list of imported CAs		X		X
Import/Export CA public keys		X		
CA Subordinate				
View		X		X
Add subordinate CAs		X		
Revoke		X		
Directory				
Bind to Directory		X	X	
Change Directory password		X	X	
View entries		X	X	X
Create, Delete, Modify entries		X	X	
User Groups				
View		X	X	X
Rename		X		
Create		X		
Delete		X		
Admin all groups		X		X
Admin any group to which they belong			X	
License Information				
View		X	X	
Modify		X		
Policy OIDs				
Admin all OIDs		X	X	X

Privilege	Trusted Roles			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Administrator**	**Security Compliance Auditor/Officer**
Queued Requests				
View queued requests		X	X	X
Modify queued requests		X	X	
Create queued requests		X		
Delete queued requests		X		
Cancel queued requests		X		
Cancel request authorization		X		
Approve request authorization		X	X	
Roles				
View		X	X	X
Modify		X		
Create		X		
Delete		X		
Admin all roles		X		X
Admin selected roles			X[1]	
Searchbases				
View		X	X	X
Modify		X		
Create		X		
Delete		X		
Admin all searchbases		X	X	X
Security Policies				
View security policies		X	X	X
Modify security policies		X		

1 End-User Roles

Privilege	Trusted Roles			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Administrator**	**Security Compliance Auditor/Officer**
Export certificate specs.		X	X	X
Import certificate specs.		X		
Export user templates		X	X	X
Import user templates		X		
Force CRLs		X		
View CRLs		X	X	X
View user policies		X	X	X
Modify user policies		X		
Create user policies		X		
User Templates				
Admin all templates		X	X	X
Users				
View		X	X	X
Add		X	X	
Re-activate		X	X	
Deactivate/Remove		X	X	
Change DN		X	X	
Modify properties		X	X	
Revoke certificates		X	X	
Update key pairs		X	X	
Set for key recovery		X	X	
Cancel key recovery		X	X	
Modify key update options		X		
View activation codes		X	X	
Users – Advanced				
Modify OIDs		X		

Privilege	Trusted Roles			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Administrator**	**Security Compliance Auditor/Officer**
Change user's role		X		
Modify group membership		X	X	
Import new users		X		
Export to another CA		X		
Archive users		X		
View archived users		X		X
Retrieve archived users		X		
Restore information to Directory		X	X	
Perform PKIX requests		X	X	
Create user profile		X		
Recover user profile	X[2]	X		
Users – Other				
View attribute certificate		X	X	
Modify attribute certificate		X	X	
Create attribute certificate		X	X	X
Delete attribute certificate		X	X	
View registration password		X		
Modify registration password		X	X	
Validate registration password		X		
Notify client		X	X	
Modify Directory properties		X	X	

The GPO PA shall enforce separation of role for sensitive PKI functions by assigning the duties of OA Officer – Master User, OA Officer – Security Officer, OA Officer – Administrator,

2 Master Users can setup Security Officers for recovery

Security Compliance Auditor/Officer and OA System Administrator to separate individuals. No individual shall have more than one of these roles.

In addition, there is separation between personnel that create policies, implement policies, perform registration, and perform audits. To ensure that no one corrupt individual may modify the operation of the CA, all security sensitive functions shall require authorization by more than one individual.

5.2.3 Number of Persons Required Per Task

All Entrust Security Officer operations need at least one Security Officer authorization. Certain functions, such as activation of the CA Private Key, will be protected by multi-person controls. The following operations need two authorizations:

- Generation of GPO-SCA Signing Keys
- Activation of GPO-SCA Signing Keys
- Using GPO-SCA Signing Keys
- Deactivation of GPO-SCA Signing Keys
- Backing up or Duplicating of GPO-SCA Private Signing Key
- Physical Control of Backups of GPO-SCA Signing Keys
- Physical Access or Control of the Cryptographic Module
- Physical Access or Control of the GPO-SCA
- Physical Access or Control of the GPO-SCA Safes and/or Secure Containers
- Physical Access to the SCA Signing Keys
- Adding and deleting Security Officers
- Setting default certificate lifetimes
- CA master key updates
- Recovery of Administrator and Officer accounts
- CA hardware, OS, and application software maintenance

5.2.4 Identification and Authentication for Each Role

Subscribers filling Trusted Roles authenticate to the CA systems using PKI credentials.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

The personnel holding GPO-SCA Trusted Roles are selected based on loyalty, trustworthiness, and integrity. All individuals filling Trusted Roles for the GPO-SCA must be U.S. citizens. Copies of documentation proving an individual's citizenship and security clearance status (if applicable), for GPO-SCA Trusted Role personnel, will be maintained by the OA, and made available during compliance audits.

In addition to the above, individuals filling Trusted Roles for the GPO-SCA will:

- Have not knowingly been previously relieved of their PKI duties or responsibilities for reasons of negligence or non-performance of duties
- Are appointed in writing by the PA or OA as appropriate
- Have not knowingly been denied a security clearance, or had a security clearance revoked
- Have not been convicted of a felony offense
- Have successfully completed an appropriate training program
- Have demonstrated the ability to perform their duties
- Are trustworthy

5.3.2 Background Check Procedures

Prospective employees for these Trusted Roles will be informed that personnel screening (e.g., references, credit checks, criminal record checks, etc.) will be conducted on any person that is being considered for such a position.

If approved by the GPO PA, an active, current GPO security clearance may be used in lieu of the personnel screening identified above.

If the trustworthiness of an individual is questioned while he or she is on the job, then the person will be removed from the sensitive position while the problem is being investigated.

5.3.3 Training Requirements

Training has been established for each individual filling a Trusted Role for the GPO-SCA, including both the requirements and operations of the role and the PKI in general. An employee that has been assigned to a Trusted Role shall not begin working in that role until the person is trained for that role. The OA is responsible for ensuring that training is accomplished for employees that serve in Trusted Roles.

Records of the training that has been provided shall be maintained on site in paper or electronic media (e.g., a text document or a spreadsheet) and shall be made available to the auditors during every compliance audit.

5.3.4 Retraining Frequency and Requirements

Any significant change to this CPS, PKI hardware or software will require retraining of affected personnel. The OA will inform individuals filling Trusted Roles for the GPO-SCA when retraining is required, and will provide any required retraining.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Any person that operates in violation of the GPO CP or the practices and procedures stated herein, whether through negligence or with malicious intent, may have privileges revoked and may be subject to administrative and disciplinary action. Repeated or significant violation of policy may result in revocation of the individual's public key certificate or a formal notification by the GPO PA to cease the operation.

5.3.7 Contracting Personnel Requirements

As stipulated in the GPO CP.

5.3.8 Documentation Supplied to Personnel

All CA operators are provided appropriate system, application and cryptographic module documents which are retained at the CA location.

At a minimum, the following documentation will be supplied:

Role	Documentation Supplied
Master Users	• Chrysalis Luna documentation (from vendor) • Entrust Security Manager Operations Guide • PA approved CP
System Administrator	• Windows 2000 on-line documentation (help files) • Entrust Security Manager Operations Guide • PA approved CP • PA approved CPS
Security Officer	• Windows 2000 on-line documentation (help files) • Entrust Security Manager Operations Guide • Entrust Security Manager Administration Guide • Chrysalis Luna documentation (from vendor) • PA approved CP • PA approved CPS
Registration Authority	• Entrust Security Manager Administration Guide • PA approved CP • PA approved CPS

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

Entrust software will initiate the process of generating the key pairs for the SCA Subscriber. Use of Federal Information Processing System (FIPS) approved cryptographic modules precludes exposure of plaintext key outside of the cryptographic modules. The SCA Subscriber's signature key pair will be generated on a FIPS 140 Level 1 or higher (the RA will be generated on a Level 2 hardware token), validated cryptographic module and the Subscriber's public signature key is delivered to the CA at that time, and the Subscriber's encryption key pair will be generated at the CA machine and the Subscriber's private decryption key will be delivered to the Subscriber at that time. For subscribers that have keys issued on hardware tokens, an authorized GPO PKI Trusted Role staff member (Security Officer or Registration Authority) shall issue the token to the subscriber.

Chrysalis-ITS LunaCA3 hardware tokens (validated for FIPS 140 Security Level 3) will be used to generate and store the GPO-SCA CA keys.

The CA key pair generation will be in compliance with PKCS#1, including the tests for primality. The private key will never be exposed outside the module in unencrypted form.

6.1.2 Private Key Delivery to Subscriber

Private signature keys will be generated and remain within the crypto boundary of the cryptographic module of the key owner, thus no delivery is required.

Private decryption keys will be delivered by the GPO-SCA using the security protection provided by PKIX-CMP.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the certificate issuer electronically in a certificate request in accordance with PKIX-CMP.

6.1.4 CA Certificates and Public Key Availability and Delivery to Entity CAs

GPO-CA certificates shall be posted in the border directory, so Entity CAs have access. The GPO PCA certificate is a self-signed certificate. The border directory shall implement access controls sufficient to prevent a certificate substitution attack.

6.1.5 Key Sizes

The GPO-SCA key modulus is 2048 bits for RSA.

Subscriber's key modulus is 1024 bits, or greater, for RSA.

The GPO-SCA uses AES-256 for database encryption.

6.1.6 Public Key Parameters Generation

As stipulated in the GPO CP.

6.1.7 Parameter Quality Checking

As stipulated in the GPO CP.

6.1.8 Subscriber Key Generation

Subscriber's signature keys shall be generated by the Subscriber (the client software or hardware being used by the Subscriber) and the encryption keys shall be generated by the CA. Both software and hardware may be used, as specified in Section 6.2.1. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved module.

6.1.9 Key Usage Purposes

Keys are certified for use in signing, non-repudiation or encrypting. Certificates used for digital signatures set the *digitalSignature* bit and the *nonRepudiation* bit. Certificates to be used for data encryption set the *keyEncipherment* bit. GPO-CA certificates shall set two key usage bits: *cRLSign* and *CertSign*.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is the latest version of the FIPS 140 series, *Security Requirements for Cryptographic Modules*.

CA signing private key storage is performed using a hardware cryptographic module that is validated to FIPS 140 Security Level 3 (or higher).

Private key storage for RA's is performed using a hardware cryptographic module that is validated to FIPS 140 Security Level 2 (or higher).

Private key storage for GPO-SCA Subscribers is performed using either hardware or software cryptographic module that is validated to FIPS 140 Security Level 1 (or higher).

Private key storage for GPO-SCA Subscribers that assert the Federal PKI Common Policy OID for id-fpki-common-hardware shall use a FIPS 140 Level 2 or higher validated cryptographic module for all private key operations.

All cryptographic modules operate such that the private asymmetric cryptographic keys are never output in plaintext (unencrypted).

6.2.2 GPO-CA Private Key Multi-Person Control

Multi-person control requires that more than one individual independently authenticate themselves to the system that will perform CA operations. This mechanism prevents any single party (CA or otherwise) from gaining access to the certificate-signing key.

The CAs private signing key, and any backup copies, are generated and stored on a hardware security module (HSM). The HSM enforces multi-person access control for the CA.

The LunaCA3 PED Keys are used to initialize and login to the LunaCA3 hardware tokens, to create clones and to enforce multi-person (M-of-N) controls. The following paragraphs describe the various PED keys and their intended uses:

Gray PED Key - The Gray PED Key is the default key used to initialize and potentially re-initialize the LunaCA3 Token. Any Gray PED Key can be used to initialize or re-initialize any Token. There will be a total of 3 Gray PED Keys. Once the key generation ceremony is complete the 3 Gray PED Keys will be secured with tamper-evident seals and securely stored by the OA.

Blue PED Key - The Luna Security Officer (LSO) PED Key is used to clone Tokens. The LSO PED Key holds the LSO PIN and is used for creating Token users and changing Token passwords. There will be a total of 3 Blue PED Keys. Once the key generation ceremony is complete, the Blue PED Keys will be secured with tamper-evident seals and securely stored by the OA.

Black PED Key - The Black PED Key is used to login to the Luna Token when starting Entrust/Authority. There will be 3 Black PED Keys. Once the key generation ceremony is complete, one Black PED Key will be held in the possession of the Luna User; the other Black PED keys will be secured with tamper-evident seals and securely stored by the OA.

Red PED Key - The Red Key, Cloning PED Key, is used to clone LunaCA3 tokens. It carries the domain identifier for the Tokens. It is created/imprinted with the first Token and then carries the domain to the other Tokens thus permitting PED Key cloning amongst only those Tokens. There will be 3 Red PED Keys. Once the key generation ceremony is complete, the 3 Red PED Keys will be secured with tamper-evident seals and securely stored by the OA.

Green PED Key - The Green PED keys are used for M of N capabilities. M of N is an optional access-restriction function to further enhance the security of LunaCA3 token operations. M of N involves an additional password or PIN, applied to the token, which must accompany the User or LSO login keys. The M of N password is a shared secret that is distributed (or split) among several Green PED keys. M of N will be 1 of 3. The shared secret will be split amongst 3 Green PED keys. There will be 1 Green PED key required at each login. Any future login to the token requires that 1 of the 3 green share keys be provided, in addition to either the blue LSO key or the black Luna User key. Once the key generation ceremony is complete 2 sets of 3 Green PED Keys will be secured with tamper-evident seals and securely stored by the OA. The 3 remaining Green PED keys will be distributed to the appropriate individuals.

The OA maintains a list of personnel that have been given access to the PED keys. The list will be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

Under no circumstances are signature keys used to support non-repudiation or digital signature services escrowed by a third party.

The GPO-SCA escrows all private encryption keys.

6.2.3.1 Escrow of CA Encryption Keys

The CA keys shall not be escrowed.

6.2.4 Private Key Backup

The HSM containing the SCA keys will be cloned in order to support the high availability CA configuration and Disaster Recovery. Cloning copies the contents of one secure cryptographic

token to another without exposing the keys outside of the HSM. The cloning procedure maintains hardware secured backups and verifiable audits through a direct hardware-to-hardware backup procedure. To prevent unauthorized use of backup materials, backup tokens maintain the same access controls as the original.

The token will be cloned 2 times to create 3 identical tokens (1 production, 1 production backup and 1 off-site backup) of the CA root keys. The initial cloning procedure will be performed as part of the key generation ceremony.

The OA periodically tests all tokens, including the clones, to ensure that they are operational. Tokens that have failed will be immediately replaced by new clones.

6.2.4.1 Backup of GPO-CA Private Signature Key

The SCA private signature keys are backed up under the same multi-person control as the creation of the original signature key. This backup/cloning procedure is completed as a formal script that specifies the detailed step-by-step procedure. The script defines the individuals that are required to complete the backup/cloning procedure and meet the multi-person control requirement.

A single copy of the signature key is securely stored at the SCA location. A second copy will be securely stored at an off-site backup location. Copies of the signature key shall be stored on cryptographic tokens and shall be placed in secure containers, and the activation information for the signature key shall be placed in a separate security container, in tamper-evident envelopes, from the cryptographic tokens.

6.2.4.2 Backup of Subscriber Private Signature Key

All Subscriber private signature keys shall be in the sole control of the Subscriber.

6.2.5 Private Key Archival

A stipulated in the GPO CP.

6.2.6 Private Key Entry Into Cryptographic Module

Private keys are generated within the cryptographic module. Use of FIPS 140 validated cryptographic modules prevents exposure of unencrypted key outside the cryptographic modules.

6.2.7 Method of Activating Private Key

The CA cryptographic module retrieves and activates the CA private signing key only when needed. The GPO-SCA private signing key is never exposed outside of the cryptographic module. Activation of the GPO-SCA private signature key requires the Black or Blue PED Key and the associated PIN in addition to one Green PED Key.

The Subscriber is authenticated to the cryptographic module before the activation of any private key. Methods of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data is protected from disclosure (i.e., the data is not displayed while it is entered).

Subscriber private keys are activated when the Subscriber logs into (i.e. authenticates to) the certificate application.

6.2.8 Method of Deactivating Private Key

The private keys remain active for the period of login. The login period is ended either by the Subscriber logging out from the certificate application or automatically as determined by a preset timer. For GPO-SCA Subscribers, the idle-timer is set to 15 minutes.

For those Subscribers using a hardware cryptographic token, the Subscriber's token will be deactivated as described above or by removing the token from the reader.

6.2.9 Method of Destroying Private Key

For those Subscribers using a hardware cryptographic token, the token is reinitialized using a vendor-supplied utility.

6.3 GOOD PRACTICES REGARDING OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The public keys are archived as part of the certificate archival.

6.3.2 Usage Periods for the Public and Private Keys

The GPO-SCA key pairs are set up for manual update. The GPO-SCA key validity period is as follows:

Key Type	Key Validity Period	Certificate Validity Period
Signature	3 years	6 years

The key validity periods for GPO-SCA Subscribers are as follows:

Key Type	Maximum Private Key Validity Period	Maximum Certificate Validity Period
Encryption	Not Applicable	2 years
Signature or Non-Repudiation	70% Certificate Lifetime	3 years

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

Activation data (biometrics, password or PIN) will be used to protect access to use of a private key. Password-type activation data (i.e. not biometric or PIN) used by the Subscribers is required to meet the following criteria:

- At least eight characters
- At least one numeric character
- At least one uppercase character
- At least one lowercase character
- At least one special character
- No repetition of the previous 12 passwords

PIN-type activation data is required to be between 4 to 8 digits in length, inclusive.

Biometric-type activation data is dependent on the manufacturer and type of biometric system in use.

CA activation data shall not be transmitted electronically over a network, and shall be controlled in accordance with CA Key Generation Ceremony documentation, which is maintained by the Policy Authority.

6.4.2 Activation Data Protection

Activation data for Subscribers is not to be written down. However, if activation data is written down, it will be secured at the level of the data that the associated cryptographic module is used to protect, and will not be stored with the cryptographic module.

Activation data will never be shared.

6.4.3 Other Aspects of Activation Data

Procedures followed to change PED Key PINs can be found in the LunaCA3 documentation.

6.5 COMPUTER SECURITY CONTROLS

The CA server instantiation is tightly controlled and audited as part of the key generation ceremony. All software loaded on the CA server is from original manufacturer distribution media.

The SCA server is built on Windows 2000 (with the current Service Pack). The Windows 2000 operating system will have the following security features enabled: identification and authentication for all users, discretionary access control, and security audit. The Windows 2000 operating system is designed and configured to provide self-protection and process isolation.

The SCA server operates with the minimal number of local accounts required. No one will be able to perform remote login. The SCA will only run the network services required to operate the CA.

6.5.1 Specific Computer Security Technical Requirements

The operating system requires authenticated logins, provides discretionary access control, audit capability, and enforces domain integrity boundaries.

The CA Software is validated FIPS 140-1 level 1 and the HSM is validated FIPS 140-1 level 3, they provide the following security technical controls:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to GPO-CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object re-use or require separation for GPO-CA random access memory
- Require use of cryptography for session communication and database security
- Archive GPO-CA history and audit data
- Require self-test security related GPO-CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanisms for keys and the GPO-CA system

6.5.2 Computer Security Rating

There is no requirement for a computer security rating.

6.6 LIFE CYCLE TECHNICAL CONTROLS

The effectiveness and appropriateness of the security settings described in this CPS are reviewed on a yearly basis. A risk and threat assessment is performed to determine if key lengths need to be increased or operational procedures modified to maintain the required level of system security.

6.6.1 System Development Controls

The CA server hardware was purchased new and is dedicated for use as the SCA within the GPO PKI. All hardware was kept in tamper-evident sealed containers, with access restricted to authorized individuals. All access to any of the PKI hardware, prior to installation in the CA facility, was manually recorded in a paper log maintained by the OA. The OA will make this log available to the Compliance Auditors during any compliance audit.

The CA software is dedicated to providing the SCA functions. Only OA-approved software has been loaded on the CA servers.

The CA hardware has been installed in the CA facility in accordance with the physical security safeguards as defined in this CPS. These physical safeguards serve to restrict access to the CA hardware to a limited number of trusted individuals. These physical safeguards in combination with the network security controls defined in this CPS restrict the ability for malicious software to be installed on the CA hardware.

RA hardware and software shall be scanned for malicious code on first use and periodically afterward.

6.6.2 Security Management Controls

The installation and configuration of the CA software is performed under very strict, scripted guidelines as part of the key generation ceremony with each step being videotaped and audited by the Compliance Auditor identified in this CPS.

The GPO follows a formal software implementation methodology whereby all PKI software upgrades and/or modifications to production systems are first installed and evaluated in a test environment. All software modifications and/or upgrades are installed in a test environment and evaluated by the OA.

At the completion of the evaluation period, the GPO OA submits to the GPO PA a digitally signed production software or hardware modification request indicating the specific hardware device, software title and version number to be modified. In addition, the report indicates the new hardware device, software title and version number, as well as a list of modifications or enhancements that the new hardware or software provides. The GPO PA is responsible for reviewing and approving the production software or hardware modification request. If the GPO PA approves the request, it will be returned to the GPO OA digitally signed by the GPO PA.

6.6.3 Life Cycle Security Ratings

There is no requirement for life cycle security ratings.

6.7 NETWORK SECURITY CONTROLS

Remote access to the GPO-SCA server via the RA interface is secured using the security features of the PKIX-CMP protocol. No other remote access is permitted and features including inbound FTP are disabled.

All unused network ports and services on the CA system are disabled. Network software present and operational on the CA system shall be necessary for the proper functioning of the CA system.

The network connection to the GPO-SCA server is protected by a firewall. The firewall policy is as follows.

With respect to GPO-SCA application server:

- With the exception of sessions initiated using the PKIX-CMP protocol disallow all other inbound initiated sessions to the production CA server
- With the exception of sessions initiated using the LDAP protocol to the LDAP Master Directory server, disallow all other outbound initiated sessions from the production CA servers

With respect to the GPO-SCA Master Directory server:

- With the exception of sessions initiated using the LDAP protocol from the GPO-SCA server, disallow all other inbound initiated sessions to the LDAP Master Directory server

- With the exception of sessions initiated using directory update protocols to the production LDAP Slave Directory servers, disallow all other outbound initiated sessions from the LDAP Master Directory server

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated in this CPS.

7. CERTIFICATE AND CARL/CRL PROFILES

7.1 CERTIFICATE PROFILE

The GPO-SCA issues X.509 Version 3 certificates and supports the following fields:

- Version: Version field is set to v3
- Signature: Identifier for the algorithm used by the GPO-SCA to sign the certificate
- Issuer: Certificate issuer (CA) Distinguished Name
- Validity: Certificate validity period - notBefore start date and notAfter end date are specified
- Subject: Certificate subject Distinguished Name
- Subject public key information: Algorithm identifier (RSA or DSA with SHA-1), and public key

For the actual format of certificates issued by the GPO SCA, see Appendix A.

Certificates issued by the GPO SCA shall conform to the Federal PKI (FPKI) X.509 Certificate and CRL Extensions Profile (FPKI-PROF).

7.1.1 Version Numbers

Certificates issued by this CA are issued with the version number set to v3.

7.1.2 Certificate Extensions

As stipulated in the GPO CP.

7.1.3 Algorithm Object Identifiers

As stipulated in the GPO CP.

7.1.4 Name Forms

As stipulated in the GPO CP.

7.1.5 Name Constraints

Name constrains are issued in CA and Cross Certificates the SCA does not issue CA or Cross Certificates.

7.1.6 Certificate Policy Object Identifier

Certificates issued by the SCA shall assert two certificate policy OIDs: 1) the GPO certificate policy OID (as stipulated in Section 1.2 of the GPO CP); and 2) one of the FPKI Common Policy OIDs (as further stipulated in Section 1.2 of the GPO CP).

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

As stipulated in the GPO CP.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

As stipulated in the GPO CP.

7.2 CARL/CRL PROFILE

For the profile of CRL and ARL issued by the GPO SCA, see Appendix A. For the profile of the CRL and ARL issued by the GPO PCA, see the GPO PCA CPS.

7.2.1 Version Numbers

As stipulated in the GPO CP.

7.2.2 CARL and CRL Entry Extensions

As stipulated in the GPO CP.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Errors, updates, or suggested changes to this CPS document shall be communicated to the OA. Such communication must include a description of the change, contact information for the person requesting the change, and an impact assessment.

Notice of all changes to this CPS that may materially impact users of this CPS (other than editorial or typographical corrections) will be provided.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

A copy of this CPS will be available to all individuals serving as Trusted Roles in this PKI.

8.3 CPS APPROVAL PROCEDURES

Changes to this document will be reviewed and approved by the PA.

The GPO PA will make the determination that this CPS complies with GPO CP. The PA will also determine if a change to this CPS is acceptable and that the changed CPS continues to comply with the GPO CP.

The PA will provide written confirmation of CPS approval, which the PA will retain and make available for inspection during compliance audits.

8.4 WAIVERS

As stipulated in the GPO CP.

APPENDIX A: Certificate and CRL Profiles

This appendix contains the profiles for the certificates and CRL issued by the SCA.

A.1 SCA CERTIFICATE FORMAT

Field	Subordinate CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	ou=GPO Root CA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	Depends on the Assurance level of the CA
Subject Distinguished Name	ou=SCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Subject Public Key Information	1024 or 2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Certificate policies	c=no; {2 16 840 1 101 3 2 1 17 1}
Basic Constraints	c=yes; cA=True; path length constraint = 0
Policy Constraints	Not Present
Authority Information Access	C=no; optional; pointer to OCSP Responder
CRL Distribution Points[1]	c = no; always present

1 The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.2 SCA CRL PROFILE FORMAT

Field	SCA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	ou= SCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 28 days
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
CRL entry extensions	
Invalidity Date	Optional
Reason Code	Always Present; Will not include certificateHold

A.3 SCA CERTIFICATE REGISTRATION DATA REQUIREMENTS

The GPO PKI Certificate Registration Form (depicted below) defines the data required to be submitted by subscribers to the GPO CA for certificate issuance.

GPO PKI Certificate Registration Form

SECTION 1.

(This section to be completed by applicant prior to in-person registration)

USER INFORMATION (Please print)			
First Name		Middle Name	
Last Name		Email Address	
Telephone #		Organization	
Address/Room Number			
Fed. Gov't-issued Picture ID Number			
Fed. Gov't-issued Picture ID Type			
Non-Fed. Gov't-issued Picture ID Number *			
Non-Fed. Gov't-issued Picture ID Type *			
Non-Fed. Gov't-issued ID Number *			
Non-Fed. Gov't-issued ID Type *			
User Signature			
User's Supervisor (Print)			
User's Supervisor Signature			
* required only when no Fed. Gov't-issued Picture ID is available			

SECTION 2.

(This section to be completed by Registration Authority at time of Registration)

RA INFORMATION (Please print)			
RA First Name		RA Last Name	
Telephone #		Email Address	
Date of Registration Request			
Fed. Gov't-issued Picture ID verified			
Non-Fed. Gov't-issued Picture ID verified *			
Non-Fed. Gov't-issued ID verified *			
* required only when no Fed. Gov't-issued Picture I.D is available			

SECTION 3.

(This section to be completed by RA & User upon completion of Registration)

PKI REGISTRATION INFORMATION (Please print)			
PKI Credential Type (software or smartcard)			
PKI Smartcard Type (if smartcard credential)			
PKI Smartcard Identifier or Serial Number			
PKI Credential Issuance Completed			
User Full DN			
RA Name (print)		User Name (print)	
Signature		Signature	
Date		Date	

APPENDIX B: ACRONYM LIST

This appendix contains a list of acronyms used in this document.

ARL	Authority Revocation List
CA	Certification Authority
	Certificate Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CPWG	Certificate Policy Working Group
CARL	Certification Authority Revocation List
CRL	Certificate Revocation List
FBCA	Federal Bridge Certification Authority
GPO	Government Printing Office
LDAP	Lightweight Directory Access Protocol
OA	Operational Authority
PA	Policy Authority
PCA	Principal Certification Authority
PKI	Public Key Infrastructure
RA	Registration Authority
SCA	Subordinate Certification Authority